CHAVEZ & GERTLER LLP
Mark A. Chavez (CA Bar No. 90858)
Nance F. Becker (CA Bar No. 99292)
42 Miller Avenue
Mill Valley, California 94941
Tel: (415) 381-5599
Fax: (415) 381-5572

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
Francis J. Balint, Jr. (admitted *pro hac vice*)
Andrew S. Friedman (admitted *pro hac vice*)
2325 E. Camelback Rd., Suite 300
Phoenix, Arizona 85016
Telephone: (602) 274-1100
Facsimile: (602) 274-1199
(fbalint@bffb.com)
(afriedman@bffb.com)

ZIMMERMAN LAW OFFICES, P.C.
Tom Zimmerman (admitted *pro hac vice*)
77 West Washington Street
Suite 1220
Chicago, Illinois 60602
Telephone: (312)440-0020
(Tom@attorneyzim.com)
(Sharon@attorneyzim.com)

Attorneys for Plaintiff Michael Edenborough
and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL EDENBOROUGH, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

ADT, LLC d/b/a ADT SECURITY SERVICES, INC. a Florida limited liability company,

Defendant.

Case No: 16-2233 JST

CLASS ACTION

NOTICE OF MOTION AND MOTION FOR CLASS CERTIFICATION; MEMORANDUM OF POINTS AND AUTHORITIES

[REDACTED]

Judge: Hon. Jon S. Tigar

Hrg. Date: March 9, 2016
Time: 2:00 p.m.

TABLE OF CONTENTS

NOTICE OF MOTION AND MOTION 1

MEMORANDUM OF POINTS AND AUTHORITIES 2

I. INTRODUCTION 2

II. STATEMENT OF EVIDENCE AND CLAIMS 3

A. The "Security Holes" In ADT's Wireless Residential Security Systems 3

B. ADT Failed To Disclose The Security Flaws In Its Wireless Systems 7

C. ADT Actively Suppressed Public Knowledge Of The Security Holes During The Class Period 8

III. ARGUMENT 14

A. The Class Is Objectively Defined And Ascertainable 14

B. The Class Is Numerous 16

C. Plaintiff's Claims Are Typical 16

D. Plaintiff Will Fairly And Adequately Protect The Interests Of The Class 17

E. Common Issues Exist That Predominate Over The Need For Any Individualized Inquiry 18

F. This Case Is Manageable As A Class Action 22

G. Class Treatment Is Superior To Individual Actions 25

IV. CONCLUSION 25

TABLE OF AUTHORITIES

Cases

All. Mortg. Co. v. Rothwell
10 Cal.4th 1226 (1995) 22

Arredondo v. Delano Farms Co.
2014 WL 5106401 (E.D. Cal. Oct. 10, 2014) 24

Baker v. Castle & Cooke Homes Hawaii, Inc. (No. 11–00616 SOM–RLP)
2014 WL 1669158 (D. Haw. Apr. 28, 2014) 19, 20, 22

Banks v. Nissan N. Am., Inc.,
301 F.R.D. 327 (N.D. Cal. 2013) 20

Bowerman v. Field Asset Services, Inc. (No. 13-CV-00057-WHO)
2015 WL 1321883 (N.D. Cal. Mar. 24, 2015) 16

Carriuolo v General Motors Co.
823 F.3d 977 (11th Cir. 2016) 23, 24

Chamberlan v. Ford Motor Co.,
223 F.R.D. 524 (N.D. Cal. 2004) 20

Collins v. DaimlerChrysler Corp.
894 So.2d 988 (Fla. Dist. Ct. App. 2004) 20, 23

Comcast Corp. v. Behrend
133 S.Ct. 1426 (2013) 23

Consolidated Rail Corp. v. Town of Hyde Park
47 F.3d 473 (2d Cir. 1995) 16

Craft v. Vanderbilt University
174 F.R.D. 396 (M.D. Tenn. 1996) 16

Datta v. Asset Recovery Sol., LLC (No. 15-CV-00188-LHK)
2016 WL 1070666 25

Elliott v. ITT Corp.,
150 F.R.D. 569 (N.D. Ill.1992) 24

Ellis v. Costco Wholesale Corp.
657 F.3d 970 (9th Cir. 2011) 17

Engalla v. Permanente Med. Grp., Inc.
15 Cal.4th 951 (1997) 20

Gen. Tel. Co. of Sw. v. Falcon
457 U.S. 147 (1982) 17

Guido v. L'Oreal, USA, Inc.
284 F.R.D. 468 (C.D. Cal. 2012) 21, 24, 25

Hanlon v. Chrysler Corp.
150 F.3d 1011 (9th Cir. 2008) 17

Hanon v. Dataproducts Corp.
976 F.2d 497 (9th Cir.1992) 16

Helmer v. Goodyear Tire & Rubber Co. (No. 12-CV-00685-RBJ-MEH)
2014 WL 1133299 (D. Colo. Mar. 21, 2014) 20

Hunt v. Check Recovery Sys., Inc.
241 F.R.D. 505 (N.D. Cal. 2007) 16, 25

In re Bridgestone/Firestone Inc. Tires Products Liability Litigation
205 F.R.D. 503 (S.D. Ind. 2001) 18

In re Mego Fin. Corp. Sec. Litig.
213 F.3d 454 (9th Cir. 2000) 17

In re Rubber Chems. Antitrust Litig.
232 F.R.D. 346 (N.D. Cal. 2005) 18

In re Sony Vaio Computer Notebook Trackpad Litig. (No. AJB09CV2109AJBMDD)
2013 WL 12116137 (S.D. Cal. Sept. 25, 2013) 25

In re Steroid Hormone Prod. Cases
181 Cal.App.4th 145 (2010) 20

In re Wells Fargo Home Mortg. Overtime Pay Litig.
571 F.3d 953 (9th Cir. 2009) 18

Johns v. Bayer Corp.
280 F.R.D. 551 (S.D. Cal. 2012) 25

Leyva v. Medline Indus. Inc.
716 F.3d 510 (9th Cir. 2013) 22

O'Connor v. Boeing N. Am., Inc.
184 F.R.D. 311 (C.D.Cal.1988) 15

Parkinson v. Hyundai Motor Am.
258 F.R.D. 580 (C.D. Cal. 2008) 20

Pulaski & Middleman. LLC v. Google, Inc.
802 F.3d 979 (9th Cir. 2015) 23

Saltzman v. Pella Corp.
257 F.R.D. 471 (N.D. Ill. 2009) 16

Saulsberry v. Meridian Fin. Serv., Inc. (No. CV146256JGBJPRX)
2016 WL 3456939 (C.D. Cal. Apr. 14, 2016) 15

Schramm v. JPMorgan Chase Bank, N.A. (No. CV09–09442)
2011 WL 5034663 (C.D.Cal. Oct.19, 2011) 22

Smilow v. Southwestern Bell Mobile Sys., Inc.
323 F.3d 32 (1st Cir. 2003) 19

Spann v. J.C. Penney Corp.
307 F.R.D. 508 (C.D. Cal. 2015) 23

Staton v. Boeing Co.
327 F.3d 938 (9th Cir. 2003) 16

Vaccarino v. Midland Nat. Life Ins. Co. (No. CV 11-5858 CAS MANX)
2013 WL 3200500 (C.D. Cal. June 17, 2013) 22

Wal-Mart Stores, Inc. v. Dukes
131 S. Ct. 2541 (2011) 18, 19

Wolin v. Jaguar Land Rover N. Am., LLC
617 F.3d 1168 (9th Cir. 2010) 18, 20, 25

Wolph v. Acer Am. Corp.
272 F.R.D. 477 (N.D. Cal. 2011) 14, 20, 21

Statutes

California Business & Professions Code §§ 17200 *et seq.* ("UCL") ..... *passim*

California Civil Code § 1709 22

California Civil Code §§ 1750 *et seq.* ("CLRA") 2, 19, 20

California Civil Code § 3343 23

Rules

FRCP 23 ..... *passim*

Other Authorities

7A Charles A. Wright, Arthur R. Miller & Mary Kay Kane
Federal Prac. & Proc.: Civil § 1778 18

FRCP 23, Adv. Comm. Notes, 1966 Am., Subdiv.(b)(3) 18

H. Newberg & A. Conte, *Newberg on Class Actions* (4th ed.) 16, 19, 24

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND TO THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE THAT Plaintiff Michael Edenborough hereby moves the Court, pursuant to Rule 23(b)(3) of the Federal Rules of Civil Procedure, to certify each cause of action in his First Amended Complaint ("FAC") for class treatment on behalf of the following class:

> All residential customers in California who paid for an ADT wireless home security system that ADT installed or caused to be installed at any time from March 18, 2012 through August 15, 2016.

Excluded are: (1) the current and former employees, officers and directors of ADT and its agents, subsidiaries, parents, successors, predecessors, and any entity in which they or their parents have a controlling interest; (2) the judge to whom this case is assigned and his immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

Plaintiff further moves for an order appointing himself as the class representative for the class defined above; appointing Chavez & Gertler LLP and attorney Mark A. Chavez as class counsel; and setting further proceedings regarding the notice to be given to the class. Oral argument is requested.

This motion is made on the grounds that each of the causes of action of the FAC satisfies the requirements for class treatment. As more fully described in the following memorandum, the class members are identifiable by specific, objective, and verifiable criteria, and the class is sufficiently numerous. Plaintiff has claims that are typical of those of the class, and Plaintiff is an adequate class representative who has retained experienced and qualified class counsel. The primary issues of law and fact are common to each member of the class and predominate over any individual issues, and class treatment is superior to individual actions.

Plaintiff bases this motion on this Notice of Motion and accompanying Memorandum of Points and Authorities; the Declarations of Mark A. Chavez, Dwight J. Duncan, Thomas J. Maronick, and Jeffrey D. Zwirn and all exhibits thereto; the exhibits designated by ADT as "Confidential" that are lodged conditionally under seal with Plaintiff's Administrative Motion re

Sealing Order; the Proposed Order; all other papers on file in this case; and such further evidence and argument as may be presented.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Defendant ADT is a leading supplier of monitored security services, serving nearly 7 million customers nationwide and touting its brand as "one of the most respected, trusted and well-known" in the industry. (ADT Form 10-K, Exh. 49.)[1] Notwithstanding those claims, ADT for years marketed and sold its wireless residential security systems without disclosing the material information that the radio signals sent by its system's wireless door and window sensors can be easily "hacked," disabled or jammed, making its customers' homes vulnerable to unwanted and undetected entry. While ADT knew of these "security holes" (discussed below) for years, it deliberately chose not to disclose them. Indeed, ADT in March 2016 admitted that "ADT is not currently aware of any public disclosures with respect to whether the signals sent from wireless peripheral sensors to alarm panels in the residential systems ADT monitors are encrypted or unencrypted." (ADT Resp. to Cheatham Interrog. No. 4, Exh. 1 at 6:4-7.) ADT's decision to maximize its profits at the expense and risk of its customers caused tens of thousands of Californians to overpay for their security systems, and unjustly enriched ADT.

The Court in its October 24, 2016 Order on ADT's motion to dismiss (ECF Doc. 57) ruled that Plaintiff's claim that ADT failed to disclose material information about its security systems, committed fraudulent omissions, and thus violated the Consumers Legal Remedies Act ("CLRA," Cal Civil Code §§ 1750 *et seq*.) and Unfair Competition Law ("UCL," Cal. Bus. & Prof. Code §§ 17200 *et seq*.) are actionable and potentially certifiable. Plaintiff, accordingly, hereby moves the Court to certify the following class with respect to each of the causes of action set out in the First Amended Complaint ("FAC") filed June 17, 2016, with limited exclusions discussed below:

[1] All exhibits to this Motion are authenticated in the supporting Declaration of Mark A. Chavez. As explained therein, and pursuant to the terms of the Protective Order entered in this matter on July 14, 2016 (ECF Doc. 38), exhibits 2A, 4, 13, 21A, 23, and 46 and an unredacted version of this Memorandum have been filed conditionally under seal pending the Court's ruling on Plaintiff's Administrative Motion re Sealing Order.

> All residential customers in California who paid for an ADT wireless home security system that ADT installed or caused to be installed at any time from March 18, 2012 through August 15, 2016.

II. STATEMENT OF EVIDENCE AND CLAIMS

A. The "Security Holes" In ADT's Wireless Residential Security Systems

Although ADT utilizes different makes and models of equipment for its residential wireless security systems, they are all functionally equivalent. Within the home, there are wireless transmitters that notify the control panel when an event has been detected by peripheral sensors. (Decl. of Pltf. Expert Jeffrey Zwirn ["Zwirn Decl."] ¶¶ 8, 9.) These events include doors opening/closing, windows opening/closing, and motion detection. (*Id.* ¶ 9.) If the system is armed, the control panel will alert ADT central monitoring when it receives an event from one of the sensors. (*Id.*; *see also*, Deposition of Ryan Petty ["Petty Dep.," Exh. 2] at 73:19-74:7; Deposition of Steve Shapiro ["Shapiro Dep.," Exh. 3] at 31:7-32:12.)

ADT's wireless residential security systems use radio signals rather than physical wires or cables to communicate within the home between (1) the sensors and (2) the control panel set. (Zwirn Decl. ¶ 9; *see also*, Petty Dep. at 73:19-74:7; Shapiro Dep. at 31:7-17.) The communications between the sensors and the home's control panel are one-way, from sensor transmitter to panel receiver unit. (Zwirn Decl. ¶ 10; *see also* Petty Dep. at 103:22-104:7; Shapiro Dep. at 32:25-33:7.) This design decision has important technical ramifications. First, sensors are unaware of the state of the system, *e.g.*, whether the system is armed. (Shapiro Dep. at 33:23-34:14.) Second, the panel has no way of querying the health of sensors, it must rely on the sensors self-reporting their health. (Zwirn Decl. ¶ 11.) Third, sensors have no way of confirming the reception of events by the panel. (Zwirn Decl. ¶ 11; Shapiro Dep. at 34:6-14.)

The last two points result in wireless communications that are inherently unreliable: the sensors cannot confirm reception of events by the panel, and the panel cannot confirm that a lack of events is expected behavior and not due to sensor failure. (*Id.*) If an event broadcast from a sensor is not received by the panel, that event is lost with no record of it having occurred. This makes jamming attacks very effective. (Zwirn Decl. ¶¶ 13, 16.)

The wireless protocols used by the sensors to communicate with the panel are also vulnerable because they provide no encryption or authentication. (Zwirn Decl. ¶ 13; *see also* Petty Dep. at 158:11-19; Shapiro Dep. at 55:22-58:16.) Because there is no encryption, an attacker can read every message sent by the sensors. (Zwirn Decl. ¶ 13.) Because there is no authentication, the panel has no way of verifying that the messages it receives are from its sensors and not from an attacker. (*Id*) In combination, this means an attacker can easily forge messages as if they were sent from the sensors, creating false events and subsequent false alarms. (*Id*.)

ADT's wireless security systems can be disrupted and disabled from outside the home in several ways using inexpensive and readily available electronic devices. (Zwirn Decl. ¶¶ 13-16; *see also* Petty Dep. at 208:4-214:18 [Exh. 2A]; JIRA Tickets, ADT00001201-1220 [Exh. 4] [redacted]; *see also* Deposition of Gary Friar ["Friar Dep.," Exh. 5] at 106:4-7, 137:118 [wireless "RF" transmissions can be interfered with]; 133:24-134:2 [admitting that "any wireless signal can be captured and retransmitted"].)

[redacted]

The specific frequencies over which ADT's sensors communicate are public information. (Zwirn Decl. ¶ 12; *see also* Petty Dep. at 155:12-25.) Because the sensors in ADT's wireless

alarm systems utilize one-way transmissions over known, fixed frequencies, the wireless peripheral transmissions can easily be interfered with or jammed from the outside to defeat the detection of unauthorized intrusions. (Zwirn Decl. ¶¶ 13, 14, 16; Petty Dep. at 105:13-19; 155:12-20; Friar Dep. at 106:4-7 & 137:118.) [redacted]

Because the peripheral signals in ADT's residential wireless systems are neither encrypted nor authenticated, the signals can be easily "spoofed," *i.e.*, they can be recorded and replayed to stand in for an otherwise tripped sensor. (Zwirn Decl. ¶¶ 13, 15; Friar Dep. at 133:24-134:2.) Hence, the wireless signal transmissions can be replayed so as to create false alarms, the intention of which would be to encourage the homeowner to disable the zone generating the false alarms or disable the entire system, allowing unauthorized intruders ready access to a home. (Zwirn Decl. ¶¶ 13, 15, 16; *see also*, Friar Dep. at 134:15-24.) The unencrypted peripheral signals can also be monitored remotely so as to learn the homeowner's patterns and determine the best times at which to enter the premises. (Zwirn Decl. ¶ 14.)

Security professionals and researchers have long known about these vulnerabilities, and have expressed concern within the industry that low-cost wireless sensors like those used by ADT preclude the application of traditional security techniques such as encryption and authentication, as well as jam detection and evasion, due to limitations on energy consumption, computational power, and communication capabilities. (Adrian Perrig, John Stankovic, and David Wagner, *Security in Wireless Networks*, 47 Communications of the ACM [Exh. 6] at 57; *see also* Merritt Maxim and David Pollino, *Wireless Security* [Exh. 7] at pp. 47-62 [discussing various threats to wireless networks including eavesdropping, jamming, data injection and modification].)

ADT witnesses have acknowledged that unprotected radio frequencies can be jammed and that anyone can listen in. (Deposition of Brenton Rothchild ["Rothchild Dep.," Exh. 8] at 40:12-41:9, 47:25-48:18; 150:24-151:18; Friar Dep. at 106:4-7, 133:24-134:2 ["Q: Could a door sensor, open door signal be recorded and replayed? A: Any wireless signal can be captured and retransmitted."); 137:11-18; Petty Dep. at 185:7-15.)

ADT personnel have attended and monitored security conferences where residential wireless security systems were shown to be vulnerable to various forms of hacking, while others have verified that certain alarm panels can detect jamming. (Petty Dep. at 21:3-25, 64:24-65:12, 176:10-17; Deposition of Taber Manning ["Manning Dep.," Exh. 9] at 26:12-32:7; *see also* ADT00020089-91 [Exh. 10]; ADT00039122-23 [Exh. 11]; ADT00040086-87 [Exh. 12]; Shapiro Dep. at 38:20-39:13.)

[redacted] ADT since 2008 has also been aware of, and actually offered to certain residential customers, systems that use two-way radio, spread-spectrum technology, or encrypted transmissions to plug the security holes inherent in the wireless peripherals used in the systems it sells to residential customers. (Friar Dep. at 103:6-8, 103:23-25, 106:8-11, 141:5-14, 142:14-20, 143:4-8; *see also* Petty Dep. at 75:22-24; ADT Power Point dated May 1, 2008 [Exh. 13]; Shapiro Dep. at 54:22-55:4, 65:9-67:3.) This alternative technology makes it more difficult to exploit the vulnerabilities in ADT's wireless residential security system. (Petty Dep. at 134:11-15 [spread spectrum makes it more difficult to jam communications]; 135:5-9 [two-way radio can enhance ability to detect whether communication was jammed].)

Consequently, ADT was not surprised when outside researcher Logan Lamb, of Oak Ridge National Labs ("ORNL"), demonstrated in his white-paper, *Home Insecurity: No Alarms, False Alarms, and SIGINT* (ADT00011177-84, Exh. 15), how one could exploit the security flaws in ADT's wireless home security systems. (Rothchild Dep. at 70:12-25 [when he reviewed Lamb's materials, "I was not surprised that he was able to create interference that would preclude a wireless sensor from sending its signal to a panel, no."]; 71:6-14 [asked whether he felt "surprised that [Lamb] was able to correlate the signals that he observed with the sensors to be

able to identify the sensor within the home," Rothchild said, "Not necessarily. I felt that that – given enough planning and forethought and observation of the home, that was a possible activity that could occur."]; 80:20-81:17 [recounting call between ADT personnel in response to Lamb's findings, and testifying that nobody on the call expressed surprise about the findings]; *see also* Manning Dep. at 169:23-170:3 [he also was "not surprise[d]" when he read Lamb's findings that he was able to intentionally interfere with wireless signals from the sensors to the panel]; Deposition of Jim Black ["Black Dep.," Exh. 14] at 72:17-25.)

Nor have any of the ADT personnel deposed been able to specifically point to any of Lamb's findings that they contend are technically inaccurate or incorrect. (*See, e.g.* Manning Dep. at 134:1-135:3 [he read the white-paper 5 to 10 times, but could not recall anything being technically incorrect]; Rothchild Dep. at 78:6-79:23; Black Dep. at 93:17-94:5.) Indeed, Mr. Manning testified that he successfully replicated the intentional jamming and replay models discussed by Lamb in his white paper. (Manning Dep. at 153:10-22.)

B. ADT Failed To Disclose The Security Flaws In Its Wireless Systems

ADT markets its wireless home security systems as providing at least the same security protection as its wired systems. According to ADT, "[a] wireless home security system gives you the features you need, plus greater flexibility." (ADT Webpages. Exh. 16 at ADT00025045.)

Although in its form contracts ADT disclosed a number of ***other*** potential vulnerabilities of its wireless residential security systems, conspicuously absent until August 2016 (*See* Exh. 17) was any disclosure of the security flaws specific to the wireless signals sent by the peripheral sensors. (*See, e.g.*, Edenborough contract, Exh. 50.) ADT disclosed only the risk associated with disrupting the ***external*** lines of communication between the alarm panel and ADT's monitoring centers – a risk shared by both wired and wireless customers. This makes that absence of any disclosure regarding the ***internal*** transmission risk unique to the lines of communication between the wireless peripheral sensors and the control panel all the more glaring.

It was not until August 2016, *almost a year after ADT was sued in the Cheatham* case, and several months after this case was filed, that ADT took any steps toward disclosure of the security flaw long known to ADT, proving the feasibility of doing so. (*See* Excerpts from "ADT

Disclosures Concerning Wireless Security Systems," Exh. 17 at 4.) For example, to its residential service contract ADT has added the following disclosure:

> THE ALARM SYSTEM WILL NOT FUNCTION IF WIRELESS COMMUNICATION FOR THE DEVICES IS IMPAIRED. THESE WIRELESS DEVICES MAY OR MAY NOT USE ENCRYPTION AND/OR AUTHENTICATION TECHNOLOGY AND ARE VULNERABLE TO INTENTIONAL OR UNINTENTIONAL INTERRUPTION, INTERCEPTION, CORRUPTION AND TAMPERING.

(*Id.*)

Similarly, since around November 2013 ADT's website stated only that ***wired*** sensors "are reliable" and "tend[] to be less susceptible to radio or electrical interference." (*Id.*) It was not until August 2016 that ADT added language explicitly addressing the security flaws raised in this litigation: the possibility of "purposeful radio or electrical interception, corruption, alteration, blockage, manipulation, tampering, imitation, and/or mimicking by a 'hacker.'" (*Id.*) Only then did ADT disclose the disadvantages of using wireless sensors, as opposed to wired sensors, as including the fact that "[r]adio frequency signals sent to and from wireless sensors may be susceptible to incidental interference, including interference from other devices that communicate using radio waves, such as baby monitors" and that "[i]t is possible that the radio frequency signals sent to and from wireless sensors could be purposefully interfered with, interrupted, intercepted, corrupted, altered, blocked, manipulated, tampered with, imitated, and/or mimicked by a 'hacker' intent on interfering with a wireless security system." (*Id.*)

C. ADT Actively Suppressed Public Knowledge Of The Security Holes During The Class Period

ADT's concealment of the security flaws was threatened in July 2014, when Mr. Lamb planned to reveal his findings about the ease with which ADT's wireless sensors could be disabled at the 2014 Black Hat Conference. (Lamb PowerPoint, ADT00013320 [Exh. 18]; *see also* Petty Dep. at 175:14-23.) ADT learned of Mr. Lamb's proposed presentation on June 26, 2014. (ADT email, ADT00039101 [Exh. 19]; *see also* Petty Dep. at 175:14-23.) ADT employee Robert Beaver received a copy of Mr. Lamb's whitepaper and other presentation materials on July 25, 2014, and he forwarded them to ADT's defense and communication teams, among other ranking executives. (Deposition of Robert Beaver ["Beaver Dep.," Exh. 20] at 37:18-41:21, and

deposition exhibits ADT00013060 & ADT00013228 ["I will schedule a call for Monday for us to formalize our thoughts and then we can schedule something else with ORNL."].)

[redacted] (ADT emails, Exh. 21, 21A at ADT00038750, ADT00010422.) ADT contacted and confidentially advised its public relations firm, Edelman, that there was "no way for [ADT] to fix the potential flaw that [Lamb] brought to life given the sheer volume of [ADT's] customer base." (DJE-00086 [Exh. 22].) [redacted]

ADT then sprang into action to preclude effective disclosure of the security holes, including setting up a clandestine CEO-level discussion with its supplier, Honeywell, through an "innocuous looking invite," and developing "a defense plan" and a "media strategy and standby statement." (Exh. 21, 21A at ADT00010421 & ADT00038750; *see also* Exh. 24 at ADT00020107 [discussing as an "imperative" the need to implement a "strawman plan for our defense and offense regarding the hack event"]; ADT00043741 [characterizing the issue as a "big deal" that will elicit "major popular press coverage" and urging a "top to top call" between ADT's and Honeywell's respective CEOs].)

The first step in ADT's "strawman plan" was to squelch Lamb's public presentation. (*See* Julie Binder email dated July 9, 2014 [Exh. 25] at ADT00014461.) To do so, ADT Vice President Julie Binder suggested that ADT "leverage" the Electronic Security Association and ADT's "local government relationships" against Lamb: "we know the Knoxville senator – to share our concerns with [ORNL] leadership about using taxpayer dollars to support this kind of activity that

could potentially put our customers lives in danger and local Knoxville jobs in jeopardy." (*Id*. at ADT00014461.) After a flurry of internal e-mails and executive conferences, ADT set off on the offensive to squelch Lamb's presentation, despite recognition that, by so doing, ADT would be shirking its own responsibility for the "security holes." As one employee put it:

> I have great concerns here in ADT going after a formally sanctioned government program that investigates privacy and security holes in critical infrastructure, as [ADT] is suggesting.
>
> ***
>
> ***This screams of ostrich-head-in-the-sand behavior where we want no one to know of our security holes and will punish those who speak of them.***
>
> ***
>
> ***Ultimately, ADT was/is responsible for selling these products with such holes.*** Punishing those who's (sic) job is to discover them isn't a good long-term strategy. ADT will end up looking like another "bad guy" company looking to just sweep these issues under the rug.

(*Id.* at ADT00014460 [emphasis added].)

ADT first contacted Lamb directly on July 9, 2014. (Exh. 26 at ADT00043828-29.) In that call, they discussed that remediation of the security flaws would likely require complete replacement of the existing firmware and hardware, and the idea of ADT partnering with Lamb to solve the noted security flaws was also suggested and well-received. (*Id.* ["We mutually agreed that identifying, partnering and solving is the ideal path for all parties ...."] Believing that ADT was amenable to working with him to fix the security holes, Lamb emailed a copy of his paper and presentation materials to ADT on July 25, 2014. (*See* Exh. 20 at ADT00013060.)

Meanwhile, behind the scenes, ADT and Honeywell were in the process of making plans to contact ORNL, Lamb's employer, to urge it to pressure Lamb to cancel his planned public presentation. (*See* Exh. 20 at ADT00013228.) As a back-up plan, ADT prepared a draft statement to send to its customers should Lamb's presentation go forward, emphasizing ADT's purported dedication to safety and security, and falsely stating that its systems could not be compromised in the real world because the demonstration was "conducted by a highly-advanced hacker in a controlled environment." (Exh. 27.) ADT also planned to direct concerned customers to a website ironically named "http://www.ADT.com/SecurityMatters." (*Id.*)

Ultimately succumbing to the weight of ADT's pressure tactics, Lamb agreed to cancel his presentation based on the (mistaken) understanding that ADT would have further discussions with him and would address or at least disclose the security flaw. (*See* ADT email [Exh. 28].) ADT's Senior Vice President and Chief Innovations Officer, Arthur Orduna, admitted that ADT "had discussions ... with [Lamb's] mgr and his mgr's mgr at Oak Ridge .... I surmise those may have influenced this action ...." (Exh. 29 at ADT00043705; *accord* ADT00014454.)

On August 1, 2014, Orduna informed ADT's Executive Leadership Team of Lamb's cancellation: "Good news – the hacker cancelled his presentation showcasing hacks of alarm systems at Defcon and Blackhat." (Exh. 30, ADT00043671.) Although Orduna intimated that Lamb "is now working directly with our Innovation and IT Sec teams on remediating what he has discovered so far regarding the vulnerabilities in our systems[]" (*id*.) he later testified that he had no knowledge either way of Lamb working with ADT to address "the vulnerabilities" of ADT's wireless residential systems. (Deposition of Arthur Orduna ["Orduna Dep.," Exh. 31] at 198:14-199:14.)

On receiving the news that the presentation would not go forward, several congratulatory e-mails were circulated within ADT. (*See* Exh. 32-33.) One (Exh. 33) reads: "This is great news indeed but we were ready for him!! Hats off to the Comms and Digital teams for assisting Arthur and the product team in the development of a very robust defense plan!" Several others from ranking ADT executives followed. (*See* Exh. 28, 34; *see also* Exh. 39 at ADT00043794 ["Great to hear"].) Edelman personnel also chimed in, exclaiming "WOW" and "That's crazy!" (Exh. 35 at ADT00025787.)

Lamb contemporaneously described the pressure brought to bear on him not to speak in a post-conference interview with National Public Radio,[2] a report for which ADT refused to comment and, later, through its Vice President of Communications, characterized as "one of the

[2] http://www.npr.org/sections/alltechconsidered/2014/08/08/338776873/when-hackers-test-for-flaws-they-might-earn-cash-or-threats

dumbest interviews I have ever heard ... trembling in the corner!!!!" (Exh. 36 at ADT00025275 & ADT00025587; *see* Deposition of Jason Shockley ["Shockley Dep., Exh. 37"] at 88:14-89:9.)

Afterward, ADT expressed relief that it was not mentioned in the NPR report (*see* Exh. 36 at ADT00025587), and it likewise declined to respond to other press inquiries regarding the cancellation of Lamb's Black Hat presentation because, "providing comment will just open up the door to more questions." (Exh. 38 at ADT00025766; *see also* Shockley Dep. at 83:22-85:2.)

When it appeared that ADT had successfully averted public disclosure of this news, it shelved the standby plans that it had developed to communicate with customers about the proven vulnerabilities of its wireless home security systems. (Petty Dep. at 46:9-15, 47:2-16; *see also* Shockley Dep. at 81:10-82:3; ADT emails [Exh. 39] at ADT00043793-94 (showing agreement within ADT not to disclose or communicate with its customers the statements it had developed to address vulnerabilities within its wireless residential alarm systems)].)

While they were dealing with the Black Hat conference, ADT and Honeywell were contacted by a Forbes reporter regarding the security holes raised in Lamb's report. (Emails, Exh. 40.) The Forbes reporter was "looking for a statement from ADT as to (1) whether [ADT was] aware of [the vulnerabilities described by Lamb] and if [Lamb's findings were] accurate; and (2) what security measure[s] [does ADT] have in place to prevent this from happening." (*Id*.) ADT Senior Director of Corporate Communications, Jason Shockley, in an e-mail circulated amongst high-ranking ADT executives, wondered do "we have a story to tell that will offset these claims?" (Exh. 21 at ADT00010426; *see also* Shockley Dep. at 20:17-24:20.) He later recommended that ADT simply provide a "blanket statement that speaks to the security measures we have in place, but point the reporter back to Honeywell." (Exh. 41 at ADT00010454 & ADT00010465; *see also* Shockley Dep. at 23:15-20.) Edelman accordingly drafted such a statement (Exh. 23 at ADT00025382-83), which Shockley then gave essentially verbatim to Forbes: "Safety and security is a top priority at ADT, and we have spent 140 years earning the trust of our customers. *** Because we have yet to see the details of this particular research, we are unable to comment on the specifics." (Exh. 42 at ADT00009846.) ADT thus again chose concealment over

disclosure of the internally-acknowledged security holes in its wireless residential monitoring systems.

Given ADT's lack of action, and the reality that ADT was not truly interested in partnering with him to solve the known vulnerabilities in its wireless residential security systems, in October 2014 Lamb advised ADT that he had agreed to an interview with ABC, to be broadcast on its "Good Morning America" program. (*See* Exh. 43.) The piece aired on November 26, 2014, and Lamb therein urged consumers to ask their security companies if they were vulnerable to undetected entry into their homes. (Exh. 44.)[3] ADT's public response, quoted in the ABC report, was nothing more than: ADT "is committed to providing our customers with continual security and technology" and "works regularly with our suppliers to enhance the security of our products."[4]

ADT found its deliberately innocuous statement effective in minimizing customer awareness, congratulating itself "call volume is low and continues to fade off." (*See* Exh. 45 at ADT00029055.) ADT also generated specific "messaging" to be used at its call centers, in which ADT claimed to be "looking into" the matter and falsely suggested that the flaw was limited to conduct by "a highly sophisticated hacker with specialized computer equipment." (*See id.* at ADT00029057.)

ADT's residential wireless security systems can in fact easily be disabled with readily available, inexpensive equipment. All of the information necessary to disable or interfere with ADT's wireless security systems is available on the Internet. (*See* Rothchild Dep. [Exh. 8] at 72:8-73:1.) It requires no more than a sixth-grade education to assemble a radio transmitter capable of jamming a radio signal. (*See* Petty Dep. at 83:16-85:10.) Indeed, ADT's own engineers recognized in December 2014 that a more elaborate "radio device with transmit functions" was "easily optioned on line at approximately $200." (Exh. 4 at ADT00001205.)

[3] The Good Morning America segment is available for viewing at https://m.youtube.com/watch?v=ZGsMQ3WyjCU, last visited December 14, 2016.

[4] *Id.* at 2:42.

[redacted] In other words, the security hole will not be fixed for existing customers because ADT would have to absorb labor costs to do so.

III. ARGUMENT

Class certification is appropriate where (1) the class is so numerous that joinder of all members is impracticable, (2) there are questions of law or fact common to the class and subclass, (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class and subclass, and (4) the representative parties will fairly and adequately protect the interests of the class and subclass. Fed. R. Civ. Proc. 23(a). In addition to those explicit requirements, "'courts have held that the class must be adequately defined and clearly ascertainable before a class action may proceed.' [Citation.]" *Wolph v. Acer Am. Corp.*, 272 F.R.D. 477, 482 (N.D. Cal. 2011). Where, as here, certification is sought pursuant to subsection 23(b)(3), the Court must also find that the questions common to the class predominate over any questions affecting only individual members, and that a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Fed. R. Civ. Proc. 23(b)(3). As demonstrated below, each of these requirements is satisfied here.

A. The Class Is Objectively Defined And Ascertainable

The proposed class consists of "all residential customers in California who paid for an ADT wireless home security system that ADT installed or caused to be installed at any time from March 18, 2012 through August 15, 2016." Excluded from the class are: (1) the current and former employees, officers and directors of ADT and its agents, subsidiaries, parents, successors, predecessors, and any entity in which they or their parents have a controlling interest; (2) the

judge to whom this case is assigned and his immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

The proposed class definition is sufficiently precise, objective and ascertainable. *See O'Connor v. Boeing N. Am., Inc.*, 184 F.R.D. 311, 319 (C.D.Cal.1988) ("A class will be found to exist if the description of the class is definite enough so that it is administratively feasible for the court to ascertain whether an individual is a member."); *Saulsberry v. Meridian Fin. Serv., Inc.*, No. CV146256JGBJPRX, 2016 WL 3456939, at *4, 14 (C.D. Cal. Apr. 14, 2016) (it is "enough that the class definition describes a set of common characteristics sufficient to allow a prospective plaintiff to identify himself or herself as having a right to recover based on the description."). This is not a case in which the defendant's products were purchased by the unknown masses. Here, membership in the class is administratively feasible based on ADT's own business records: indeed, ADT has already identified from its "MASterMind" database and business records [redacted] current and former residential customers in California who, during the class period, purchased home security systems from ADT or an ADT dealer and have "exclusively" wireless systems; an additional [redacted] customers who "likely" have wireless sensors; and [redacted] customers who "may" have wireless sensors. (Exh. 46, ADT00049604.)[5]

As detailed in the Declaration of Plaintiff's expert Jeffrey D. Zwirn, there are several reasonable methods by which ADT's records can be used to determine which of the customers identified as "likely" or "unknown" to have wireless components in fact do so. Those methods include a database search to identify the make and model of the control panel and/or the number of "zones" (because each sensor in a wireless system is its own zone, wireless systems typically have significantly more zones than wired systems), to records of "low battery" reports, which are

[5] "Exclusively wireless" customers are those who have a specific, exclusively wireless alarm control panel. (Friar Depo. [Exh. 5] at 70:2-9.) "Likely wireless" customers are those who "have integrated wireless receivers and ship as a kit with wireless devices." (*Id*. at 70:21-71:1.) "Unknown" customers are those whose panels are designed for a wireless system, but may have a wireless receiver added as a stand-alone or integrated system. (*Id*. at 73:8-18.)

also indicative of wireless systems. (Zwirn Decl. ¶¶ 17-26.) To whatever extent ADT's business records are inconclusive,[6] membership is susceptible to simple, objective proof, such as a photograph submitted by those class members – over 95% of whom know whether their system has some wireless components. (*Id.* ¶18; Maronick Decl. ¶ 14.)[7] ADT's alleged uncertainty as to the identity of some class members is, thus, no barrier to class certification.

B. The Class Is Numerous

The almost [redacted] California customers ADT has identified as having "exclusively" wireless systems is, alone, more than sufficient to satisfy Rule 23's requirement that the class be "numerous" and that joinder of all members be "impracticable." *See, e.g., Staton v. Boeing Co.*, 327 F.3d 938, 953 (9th Cir.2003) (class of 15,000 met numerosity requirement); *Consol. Rail Corp. v. Town of Hyde Park*, 47 F.3d 473, 483 (2d Cir. 1995) (numerosity presumed where class consists of forty or more members); H. Newberg & A. Conte, *Newberg on Class Actions* (4th ed.) § 24.18.

C. Plaintiff's Claims Are Typical

A plaintiff's claim "is typical if it arises from the same event or practice or course of conduct that gives rise to the claims of other class members and his or her claims are based on the same legal theory." *Hunt v. Check Recovery Sys., Inc.*, 241 F.R.D. 505, 511 (N.D. Cal. 2007) (quot. marks and citations omitted); *see also Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir.1992) ("Typicality refers to the nature of the claim or defense of the class representative, and not to the specific facts from which it arose[.]") (citations and quot. marks omitted). To be found typical, a plaintiff must show that other class members have been similarly injured by the same course of conduct that is not unique to the named plaintiff. *Ellis v. Costco Wholesale Corp.*,

---

[6] To the extent ADT's lack of business records causes difficulties in proving class membership, the burden shifts to ADT to disprove class membership of those customers who utilize hybrid control panels. *See Craft v. Vanderbilt University*, 174 F.R.D. 396 (M.D. Tenn. 1996).

[7] *See, e.g., Saltzman v. Pella Corp.*, 257 F.R.D. 471, 475-6 (N.D. Ill. 2009), *aff'd*, 606 F.3d 391 (7th Cir. 2010) (if defendant's records are insufficient for determining owners of defendant's products, class members can be identified through "a combination of the use of sales records, publication of notice, and verification by photograph"); *see generally, Bowerman v. Field Asset Services, Inc.*, 13-CV-00057-WHO, 2015 WL 1321883, at *8 (N.D. Cal. Mar. 24, 2015) ("That the class may have to be ascertained through a combination of evidentiary sources does not necessarily mean that ascertaining it is administratively infeasible.").

657 F.3d 970, 984 (9th Cir. 2011). However, representative claims "need not be substantially identical;" they are "typical" so long as they are "reasonably co-extensive with those of absent class members." *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1020 (9th Cir. 2008.) Typicality is, thus, generally satisfied if the named plaintiff is a part of the class and has suffered the same injury as other class members. *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 156 (1982).

Plaintiff Edenborough is part of the class he seeks to represent because he is a victim of ADT's uniform failure to disclose the risks associated with the wireless home security systems that ADT sold him and other class members. After purchasing his home in Oakland in March 2012, he contacted ADT, met with a sales representative, purchased an ADT wireless security system, and had the ADT equipment installed. (Edenborough Dep. [Exh. 50] at 9:17-19, 41:12-22.) He relied on ADT's reputation and expertise, and was unaware of the security risks of ADT's wireless system when he purchased it. (*Id*. at 42:20-23, 55:18-56:4, 89:19-90:7, 91:17-21, 92:4-9.) Had he known the risks, he would have ordered a wired system or searched for a more secure system. (*Id*. at 42:24-43:6, 53:3-14.) Notably, ADT has asserted no defense against Plaintiff not also asserted against the Class. (*See* ADT Answer to FAC, ECF Doc. 71.)

Edenborough became a plaintiff because "I have a faulty system that wasn't revealed to me at the time of my purchase." (*Id*. at 22:7-11.) He has been damaged because "I have been paying all these years for a system that wasn't disclosed that it's hackable." (*Id*. at 128:5-10.) ADT cannot dispute that each class member was injured by the same course of conduct – namely, its failure to disclose the risks associated with wireless home security systems. ADT's defenses – that there is no risk and that even if there were a risk, it was sufficiently disclosed – apply class-wide and are not unique to Plaintiff. Accordingly, Plaintiff's claims are typical.

D. Plaintiff Will Fairly And Adequately Protect The Interests Of The Class

The adequacy requirement is satisfied if the class representative will fairly and adequately protect the interests of the class. Fed. R. Civ. P. 23(a)(4). This requires that the plaintiff have no conflict of interest with the proposed class and be represented by competent counsel. *In re Mego Fin. Corp. Sec. Litig*., 213 F.3d 454, 462 (9th Cir.2000); *Hanlon,* 150 F.3d at 1020; *Ellis*, 657 F.3d 970 at 985 (adequacy depends on "an absence of antagonism between representatives and

absentees, and a sharing of interest between representatives and absentees"); *In re Rubber Chem. Antitrust Litig.*, 232 F.R.D. 346, 351 (N.D. Cal. 2005).

Here, there is no conflict between Plaintiff and the members of the class. Edenborough is a member of the class and has suffered the same or similar injuries as the rest of the class. He has agreed to prosecute this case vigorously on behalf of the class, and he has retained qualified counsel to do so. (Chavez Decl. ¶¶ 2-16; Exh. 51 [Zimmerman Law], 52 [Bonnett Fairbourn].) He understands that he is a class representative and has agreed to undertake the attendant obligations. (*Id*. at 60:8-10, 60:16-19, 61:14-20.) He is a more than adequate class representative.

E. Common Issues Exist That Predominate Over The Need For Any Individualized Inquiry

"Commonality exists where class members' situations share a common issue of law or fact, and are sufficiently parallel to insure a vigorous and full presentation of all claims for relief." *Wolin v. Jaguar Land Rover N. Am., LLC,* 617 F.3d 1168, 1172 (9th Cir. 2010). "[E]ven a single common question will do." *Wal-Mart Stores, Inc. v. Dukes*, 546 U.S. 338, 359 (2011). "What matters to class certification ... is not the raising of common 'questions' – even in droves – but rather the capacity of a class-wide proceeding to generate common ***answers*** apt to drive the resolution of the litigation." *Id*., 564 U.S. at 350 (emph. orig., cit. omitted); *see generally* Fed. R. Civ. P. 23, Adv. Comm. Notes, 1966 Am., Subdiv.(b)(3) ("fraud perpetrated on numerous persons by the use of similar misrepresentations may be an appealing situation for a class action").

As for predominance, "Rule 23(b)(3) asks whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *In re Wells Fargo Home Mortg. Overtime Pay Litig.*, 571 F.3d 953, 957 (9th Cir.2009) (internal quot. marks and citation omitted). Common questions predominate whenever they "present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication." 7A Charles A. Wright, Arthur R. Miller & Mary Kay Kane, *Federal Prac. & Proc.: Civil* § 1778; *see also In re Bridgestone/ Firestone Inc. Tires Products Liability Litig.*, 205 F.R.D. 503, 520 (S.D. Ind. 2001).

Even where substantial individualized factual determinations may be necessary, common questions predominate if those individualized determinations are nonetheless susceptible to

generalized proof such as design documents and business records. *Newberg on Class Actions* § 4:50 (5th ed.) (common issues predominate when "individual factual determinations can be accomplished using computer records, clerical assistance, and objective criteria – thus rendering unnecessary an evidentiary hearing on each claim"); *see also Smilow v. Southwestern Bell Mobile Sys., Inc.*, 323 F.3d 32, 40 (1st Cir. 2003).

It is clear that common questions exist here. The principal issues in this case include:

(i) whether ADT's wireless home security systems are unencrypted and/or otherwise vulnerable to attack by unauthorized third parties;

(ii) whether ADT disclosed these vulnerabilities to consumers during the class period;

(iii) whether these vulnerabilities are material;

(iv) whether ADT's omissions were unfair and deceptive and thus and violate the CLRA;

(v) whether ADT has committed any unlawful, unfair and/or deceptive business practices in violation of the UCL;

(vi) whether Plaintiff and the proposed class were damaged as a result of ADT's conduct alleged herein; and

(vii) whether ADT was unjustly enriched at the expense of Plaintiff and the proposed class.

A further common question, presented by ADT's alleged First Affirmative Defense, is whether "[t]he claims asserted by Plaintiff and/or the proposed class are barred or limited in whole or in part by contractual limitations of liability contained in their Alarm Services Contract with ADT, including but not limited to the Contract's integration clause, and those limitations stated in the section of the Contract entitled, "Important Terms and Conditions." (Answer to FAC, ECF Doc. 71 at 24.)

Numerous cases have held that questions such as whether a manufacturer/seller had a duty to disclose information about problems with its products and whether the omitted facts are material are common questions that support class certification. A finding that ADT had a duty to disclose (or not), and that it violated the duty (or not), will provide a "common answer [] apt to drive the resolution of th[is] litigation." *Wal-Mart*, 564 U.S. at 350; *see also Baker v. Castle & Cooke Homes Hawaii, Inc.*, No. CIV. 11-00616 SOM, 2014 WL 1669158, at *5 (D. Haw. Apr.

28, 2014) (commonality requirement is satisfied where every claim depends on the resolution of the threshold question of whether a defect exists or not); *Helmer v. Goodyear Tire & Rubber Co.*, No. 12-CV-00685-RBJ-MEH, 2014 WL 1133299, at *5 (D. Colo. Mar. 21, 2014) (commonality satisfied because "asking a fact-finder to decide whether the product is indeed defective in the way that the plaintiffs allege would 'generate common answers apt to drive the resolution of the litigation.'").

These common questions also predominate. Whether or not ADT had a duty to disclose is a predominant common question. *Wolin*, 617 F.3d at 1173 ("Common issues predominate such as whether Land Rover was aware of the existence of the alleged defect, whether Land Rover had a duty to disclose its knowledge and whether it violated consumer protection laws when it failed to do so."); *Banks v. Nissan N. Am., Inc.*, 301 F.R.D. 327, 335 (N.D. Cal. 2013); *Keegan v. Am. Honda Motor Co.*, 284 F.R.D. 504, 532 (C.D. Cal. 2012) (CLRA claims), 534 (UCL claims), 537 (warranty claims) (C.D. Cal. 2012); *Parkinson v. Hyundai Motor Am.*, 258 F.R.D. 580, 596-97 (C.D. Cal. 2008); *Chamberlan v. Ford Motor Co.*, 223 F.R.D. 524, 526-27 (N.D. Cal. 2004) (predominating common questions "include whether the design of the plastic intake manifold was defective, whether Ford was aware of the alleged design defects, whether Ford had a duty to disclose its knowledge, whether it failed to do so, whether the facts that Ford allegedly failed to disclose were material, and whether the alleged failure to disclose violated the CLRA.").

Moreover, reliance on ADT's omissions may be presumed if the omission is material; with materiality, in turn, based on an objective standard that is susceptible to common proof. *Wolph*, 272 F.R.D. at 488; *accord Collins v. eMachines, Inc.*, 202 Cal.App.4th 249, 256 (2011), *as modified* Dec. 28, 2011 ("In the CLRA context, a fact is deemed 'material,' and obligates an exclusively knowledgeable defendant to disclose it, if a 'reasonable [consumer]' would deem it important in determining how to act in the transaction at issue."); *In re Steroid Hormone Prod. Cases*, 181 Cal.App.4th 145, 157 (2010), *as mod.* Feb. 8, 2010; *see also Engalla v. Permanente Med. Grp., Inc.*, 15 Cal.4th 951, 977 (1997), *as mod.* July 30, 1997 ("A misrepresentation is judged to be 'material' if 'a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question.'"); *Guido v.*

L'Oreal, USA, Inc. 284 F.R.D. 468, 481, (C.D. Cal. 2012), *reconsidered on other grounds* (C.D. Cal., June 25, 2012, No. CV 11-1067 CAS JCX) 2012 WL 2458118 (certifying as class action claims that defendant omitted material information about its products which, if disclosed, would have caused consumers to pay less or not to purchase the product at all, and holding that "Whether defendants' alleged omissions and misrepresentations violated the UCL, CLRA, [and other statutes] present common factual and legal issues.")

While ADT contends it disclosed the risks of its security systems in the contracts provided to its customers, common evidence will prove the lack of any effective disclosure. As discussed on page 7, above, the disclosures in ADT's standard form contracts used during the class period relate to the risks associated with cutting the lines of external communication *between the alarm panel and ADT's monitoring centers*; not cutting the internal lines of communication *between the security sensors and the alarm panel*, which is the issue here. Indeed, ADT in March 2016 acknowledged that it was itself unaware "of any public disclosures with respect to whether the signals sent from wireless peripheral sensors to alarm panels in the residential systems that ADT monitors are encrypted or unencrypted." (Exh. 1 at 6:4-7.) Using well-established survey protocol, Plaintiff's expert Professor Thomas Maronick has conducted a nationwide survey indicating that well over 90% of ADT customers nationwide do not realize that their ADT wireless residential security system is unprotected from being electronically disabled or jammed from outside the residence (Maronick Decl. ¶ 17), and that the overwhelming majority of consumers either would not have purchased their system if the risks had been disclosed (43.4%), or would have paid considerably less (48-58.2%) (*id.* ¶¶ 19-20). Those who paid to have their system installed said they would pay 10-30% less than they are currently paying (*id.* ¶ 21).

Further, as discussed above, common evidence will also establish that ADT made a deliberate decision to withhold disclosure of the security flaws inherent in its residential wireless systems, for fear that disclosure would adversely affect its sales and brand. The scope of ADT's ramped up response to the Lamb report and attendant publicity demonstrates that ADT itself deemed the information about the "security holes" in its systems highly material to its sales.

By contrast, the only potential individualized inquiries relate to the extent of damages. This is not, however, a factor in determining whether common issues predominate. *Leyva v. Medline Indus. Inc.*, 716 F.3d 510, 514 (9th Cir. 2013) ("the presence of individualized damages cannot, by itself, defeat class certification under Rule 23(b)(3)").

Finally, ADT's discovery affirmative defense is, likewise, no bar to class certification in an omissions case such as this. "The Ninth Circuit has multiple times ... [held] that individual questions about when class members actually discovered or 'should have discovered' the elements of their claims do not predominate where, as here, plaintiffs' theory is that defendant's own omissions or deception resulted in plaintiffs remaining unaware about their injury or its cause." *Vaccarino v. Midland Nat. Life Ins. Co.*, CV 11-5858 CAS MANX, 2013 WL 3200500, at *15 (C.D. Cal. June 17, 2013) (citing, *inter alia, Cameron v. E.M. Adams & Co.*, 547 F.2d 473, 478 (9th Cir.1976) and *Williams v. Sinclair*, 529 F.2d 1383, 1388 (9th Cir.1975)); *see also Schramm v. JPMorgan Chase Bank, N.A.*, CV09–09442, 2011 WL 5034663, *11–12 (C.D.Cal. Oct.19, 2011) (noting that "[c]ourts have been nearly unanimous" in so finding).[8]

F. This Case is Manageable as a Class Action

As demonstrated above, the questions of liability in this case can all be determined through common proof. As to damages, the need to calculate the damages to be awarded to class members – out-of-pocket expenses as well as loss of the benefit of the bargain – does not create individualized issues that would render trial unmanageable.

Under California law, "[t]here are two measures of damages for fraud: out-of-pocket and benefit of the bargain." *All. Mortg. Co. v. Rothwell*, 10 Cal.4th 1226, 1240 (1995); *see* Cal. Civ. Code § 1709 ("One who willfully deceives another with intent to induce him to alter his position to his injury or risk, is liable for any damage which he thereby suffers.") For consumer fraud, a

[8] In the *Cameron* case, the Ninth Circuit held that "the presence of individual issues of compliance with the statute of limitations here does not defeat the predominance of the common questions" (547 F.2d at 478). *See also Baker v. Castle & Cooke Homes Hawaii, Inc.*, No. 11–00616 SOM–RLP, 2014 WL 1669158 at *14 (D. Haw. Apr. 28, 2014) ("When there is no reason to suspect that potential class members have or will discover product defects at significantly different times, the presence of a statute of limitations provision, by itself, is insufficient reason to compel all potential class members to pursue their claims individually.").

plaintiff may recover all such damages, including the consideration paid under the contract and out-of-pocket expenses. Cal. Civ. Code § 1780(a)(1)-(5); *see also* Cal. Civ. Code § 3343 ("One defrauded in the purchase, sale or exchange of property is entitled to recover the difference between the actual value of that with which the defrauded person parted and the actual value of that which he received ....").

Plaintiff has retained experts to determine and opine on class-wide damages under methodologies consonant with his theories of liability in accordance with *Comcast Corp. v. Behrend*, 133 S.Ct. 1426, 1435 (2013). *Comcast* does not require anything more than that the damages methodology be aligned with the theory of liability. *Pulaski & Middleman. LLC v. Google, Inc.*, 802 F.3d 979, 987 (9th Cir. 2015). Moreover, it is not necessary to demonstrate at the certification stage that the proposed methodology "will work with certainty at this time." *Spann v. J.C. Penney Corp.*, 307 F.R.D. 508, 529 (C.D. Cal. 2015), *modified*, 314 F.R.D. 312 (C.D. Cal. 2016).

It is well-recognized that a consumer class may recover under an out-of-pocket theory where a seller's misrepresentation allowed it "to command a price premium and to overcharge customers systematically." *Carriuolo v General Motors Co.*, 823 F.3d 977, 987 (11th Cir. 2016). In *Carriuolo*, the Eleventh Circuit rejected the seller's argument that differences in the perceived worth of misrepresented safety ratings precluded class certification, reasoning that, "[a]s long as a reasonable customer will pay more for a vehicle with perfect safety ratings, the dealer can hold out for a higher price than he would otherwise accept for a vehicle with no safety rating:"

> [B]ecause a vehicle with three perfect safety ratings may be able to attract greater market demand than a vehicle with no safety ratings, the misleading sticker arguably was the direct cause of actual damages for the certified class even if members individually value safety ratings differently.

823 F.3d at 987; *see also, Collins v. DaimlerChrysler Corp.*, 894 So.2d 988, 991 (Fla. Dist. Ct. App. 2004) ("Is a car with defective seatbelt buckles worth less than a car with operational seatbelt buckles? Common sense indicates that it is[.]").

The same rationale applies here, only more so: a security system with a "security hole" of unprotected and easily jammable wireless signals is worth less than an encrypted (or otherwise

protected) security system. ADT's promotion of its wireless residential security system allowed it "to command a price premium," the size of which can be determined on a class-wide basis. *Carriuolo*, 823 F.3d at 987. Professor Maronick's survey confirms that, while a large percentage of ADT customers would drop the system altogether had they known of the security flaw, over 80% of those ADT customers who would not drop the wireless security system altogether would only pay 10-30% less for an unprotected system, with another 10% requiring an even greater discount. (Maronick Decl. ¶ 21 and Table 9.)

The declaration of Plaintiff's damages expert Dwight Duncan further demonstrates that there are several viable methodologies by which overcharge damages can be quantified on a class-wide basis consistent with Plaintiff's non-disclosure theory of liability. (Duncan Decl. ¶¶ 3, 8-32.) *See Guido v. L'Oreal, USA, Inc.*, Nos. 2:11–CV–01067 CAS (JCx), 2:11–CV–05465 CAS (JCx), 2014 WL 6603730, *8 (C.D. Cal. July 24, 2014) (plaintiffs need not show on class certification that they paid a premium due to the alleged misconduct; "they must merely provide a method for calculating that premium on a classwide basis"). Damages can also be calculated on a theory of unjust enrichment based on ADT's business records (*id.*, ¶¶ 3, 33-34) or, as a last resort, using the liquidated damages provisions that ADT itself set forth in its form contracts (*id.* ¶¶ 3, 35). Specifically, ADT's contracts (*e.g.* Edenborough Dep. Exh. 33 [Motion Exh. 50]) provide that if it is found liable for damage under any legal theory notwithstanding its purported contractual disclaimers, ADT's liability shall be limited to "10% of the annual service charge or $500, whichever is greater." In any event, the better course to follow with regard to the calculation of damages would be to wait until the common questions have first been resolved. *Elliott v. ITT Corp.*, 150 F.R.D. 569, 575 (N.D. Ill.1992) *report and rec. adopted*, 150 B.R. 36 (N.D. Ill. 1992) ("Normally, the question of injury to individual class members is deferred until after resolution of the common questions."); *Newberg on Class Actions* §4:26 ("[t]he 'risk [that individual damage calculations will be unmanageable] is better addressed down the road, if necessary' by altering or amending the class, not by denying certification at the outset."); *accord*, *Arredondo v. Delano Farms Co.*, 2014 WL 5106401, at *7 (E.D. Cal. Oct. 10, 2014).

G. Class Treatment is Superior to Individual Actions

Though ADT might contend in opposition that a class action is not superior to individual actions because class members could bring individual claims, courts have generally found that "[j]udicial economy weighs in favor of a class action where, as here, liability turns on whether [defendant's conduct was] ... false or misleading." *Johns v. Bayer Corp.*, 280 F.R.D. 551, 559 (S.D. Cal. 2012); *see also In re Sony Vaio Computer Notebook Trackpad Litig.*, No. AJB09CV2109AJBMDD, 2013 WL 12116137, at *20 (S.D. Cal. Sept. 25, 2013) (resolving the question regarding the existence of a design defect, "one way or another, for hundreds of thousands of VAIO computers sold since 2006, adds great economy of scale favoring class action treatment"). This is particularly true for class actions, like the present action, that seek to enforce compliance with consumer protection laws. *Guido*, 284 F.R.D. at 484.

Moreover, it would be economically infeasible for class members to pursue their claims individually given that the expense of such litigation would be exponentially larger than the amount in controversy for any individual consumer. *Id*.; *Keegan,* 284 F.R.D. at 549; *see also Wolin*, 617 F.3d at 1176. This is particularly apt here, where many class members will be unaware of their rights due to ADT's ongoing failure to disclose. A class action is, therefore, superior to any alternative methods of adjudication available in this case. *Datta v. Asset Recovery Sol., LLC*, No. 15-CV-00188-LHK, 2016 WL 1070666, at *8 (N.D. Cal. Mar. 18, 2016) (class action superior where "many class members ... are likely unaware of their rights and [thereby] unlikely to sue individually"); *see also Hunt v. Check Recovery Sys., supra*, 241 F.R.D. at 514.)

IV. CONCLUSION

For all the foregoing reasons, Plaintiff requests that the Court grant this motion and enter the accompanying proposed order certifying the causes of action in the FAC for class treatment.

Respectfully submitted,

Dated: December 14, 2016

CHAVEZ & GERTLER LLP

By: _____

Mark A. Chavez

Attorneys for Plaintiff and the Proposed Class